iGovernment

Prins, J.E.J.; Broeders, D.; Griffioen, H.

Published in:
Computer Law and Security Review

Publication date:
2012

Document Version
Publisher's PDF, also known as Version of record

AUTHOR QUERY FORM

ELSEVIER	**Journal:** CLSR **Article Number:** 4666	**Please e-mail or fax your responses and any corrections to:** **E-mail: S.J.Saxby@soton.ac.uk** **Fax: +44 (0) 23 8059 3024**

Dear Author,

Please check your proof carefully and mark all corrections at the appropriate place in the proof (e.g., by using on-screen annotation in the PDF file) or compile them in a separate list. Note: if you opt to annotate the file with software other than Adobe Reader then please also highlight the appropriate place in the PDF file. To ensure fast publication of your paper please return your corrections within 48 hours.

For correction or revision of any artwork, please consult http://www.elsevier.com/artworkinstructions.

Any queries or remarks that have arisen during the processing of your manuscript are listed below and highlighted by flags in the proof.

Location in article	Query / Remark: Click on the Q link to find the query's location in text Please insert your reply or correction at the corresponding line in the proof
Q1	Please check that the affiliations link the authors with their correct departments, institutions, and locations, and correct if necessary.
Q2	Please confirm that given names and surnames have been identified correctly.

Thank you for your assistance.

COMPUTER LAW & SECURITY REVIEW XXX (2012) 1–10

Available online at www.sciencedirect.com

SciVerse ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

iGovernment: A new perspective on the future of government digitisation☆

J.E.J. Prins[a,b], D. Broeders[b,c], H.M. Griffioen[b,d]

[a] Tilburg Institute for Law, Technology, and Society, Tilburg University, The Netherlands
[b] Scientific Council for Government Policy (WRR), The Hague, The Netherlands
[c] Department of Sociology, Erasmus University Rotterdam, The Netherlands
[d] Faculty of Law, Leiden University, The Netherlands

Keywords:
iGovernment
eGovernment
Information flows
Surveillance
Public trust
Citizen services

ABSTRACT

Innovative use of ICT applications is rapidly becoming a cornerstone of modern government policy in every area of service, care and control. Looking beyond the individual applications and layers of digitisation, we find a hodgepodge of information flows running within and between the various public authorities, policy domains, and crossing the public/private boundary. This has consequences for the relation between government and citizens. Step by step, decision by decision, the everyday work of government is changing 'the rules of the game' and giving rise to "information Government" (*iGovernment*), without this being based on any overall strategic agenda or awareness among political decision-makers. This article places this development in a new framework and suggests a perspective on a necessary paradigm shift.

1. Introduction

Modern ICT offers government many promising opportunities to speed up work processes, increase the effectiveness and efficiency of policy, offer better and more customised services, and lighten the load of bureaucracy. Under the banner of the eGovernment, ICT has been introduced to make government streamlined, digital and service-minded while at the same time catering to the needs of the citizen and "client". More recently, ICT is increasingly being used in policymaking in the care sector and in the interest of public safety and international security. Innovative use of new technologies is rapidly becoming a cornerstone of modern government policy in every area of service, care and control.

At the same time, the dynamic nature of ICT changes the "rules of the game" and thus influences the interaction between government and the citizen, between different government organisations, and between government and business. Information flows between various government organisations sometimes crosses the boundaries between the public and private sectors. Given the vast quantities of information stored and collected, governments increasingly base their dealings with citizens on categorisations and profiles, leaving those same citizens powerless and empty-handed in instances where the information turns out to be incorrect or incorrectly interpreted. Furthermore, government is often seemingly unwilling or unable to set limits to its own appetite for collecting data: it is much more likely to find reasons to gather more information than to curb its own curiosity. However, when it comes to new technology and, in particular, the information flows that new technology generates, government has a double responsibility. Government must find a way to navigate between the contrasting demands of using ICT innovatively in policy and policy implementation, and protecting citizens against the foreseen

☆ This article is based on a 2011 Dutch report entitled iOverheid. The report was written by the Scientific Council for Government Policy (Wetenschappelijke Raad voor het Regeringsbeleid – WRR), an independent scientific advisory body to the Dutch government. It was published in English as: J.E.J. Prins, D. Broeders, H. Griffioen, A.G Keizer & E. Keymolen, *iGovernment*, Amsterdam University Press 2011.

0267-3649/$ – see front matter
doi:10.1016/j.clsr.2012.03.010

Please cite this article in press as: Prins JEJ, et al., iGovernment: A new perspective on the future of government digitisation, Computer Law & Security Review (2012), doi:10.1016/j.clsr.2012.03.010

and unforeseen effects of ICT, in particular those related to complex information flows.

This article places the rapid developments within governments in the information age in a new framework, that challenges that of eGovernment, i.e. the main framework in which government now relates to ICT. We will argue that empirical developments in the realm of government and ICT reveal the limits of the eGovernment paradigm and then shift our focus to a different perspective, which we refer to here as iGovernment. This new perspective raises pointed and urgent questions that have so far not received the attention due to them. By zeroing in on the *information* Government, we focus on the information flows rather than the individual technologies and applications which are the building blocks of eGovernment and show that, far from being "engineered" by politicians and policymakers, iGovernment is in fact "emerging" in a very real and empirical sense. This raises questions about how iGovernment is to evolve further and about the relationship between the citizen and government within that context.

2. eGovernment

2.1. *The rise of eGovernment*

In the early days of eGovernment, in the early 1990s, governments regarded ICT primarily as a tool for streamlining their own (internal) organisation and processes, in particular with respect to policy implementation. Under the "eGovernment" banner, ICT quickly became all-pervasive and the emphasis gradually shifted from the internal organisation to the "outside", i.e. to policies aimed at increasing the effectiveness and efficiency of services delivered to citizens and businesses.[1] eGovernment plans and strategic agendas typically presented a positive view of new technology[2] and policymakers placed a high trust in the promise of digitisation. ICT was essentially regarded as a neutral tool that could be used to achieve certain policy aims faster, better and more efficiently without seriously influencing or changing the primary policy process. As a result there was generally little concern for the context in which ICT and eGovernment programmes were being introduced, or for the foreseeable and unforeseen effects that the use of new technologies often entails.[3] Technology was "rolled out", work processes were "streamlined" and services were "updated". "Techno-trust" prevailed.[4]

With the steady growth of government ICT over the years there were growing concerns regarding the interaction, coordination and coherence of the various systems that proliferated in the back office of government, specifically with respect to service provision.[5] These concerns focused mainly on the technical aspects, such as interoperability and open standards, and much less on the implications of a fast growing network of data and information sources. Neither was there much discussion on the dependencies and vulnerabilities created by the interoperability of digital information and on the implications of coordinating, networking and exchange of data between organisations. When vulnerabilities at the level of information architecture and exchange were acknowledged, they were sometimes immediately countered with new forms of technological "neutralisation": technology itself was put forward to neutralise the risks associated with technology. "Privacy by design" and "privacy enhancing technologies" (PETs) became new buzzwords to deal with the side effects of digitisation, such as the loss of privacy.[6]

Because politicians often lacked the resolve to see the implementation of such policies through, they have not turned out to be the solutions that they might have been.[7] The focus on technology and applications also resulted in a case-by-case approach to the digitisation of government services by politicians and policymakers. Each new digital tool, database and application was debated and decided upon in isolation of the many other initiatives in neighbouring policy domains and government organisations. eGovernment was firmly built on the idea of improving government services – transforming citizens into consumers in the passing – and using the building blocks of a myriad of separate technological applications and innovations. The resulting information structures and networks, and the organisational and social consequences thereof, were much less of a concern to the policymakers that built it.

2.2. *The limits of the eGovernment perspective*

If we look beyond the individual applications and layers of digitisation introduced within the context of eGovernment, we find a hodgepodge of information flows running within and between various government authorities. It is extremely rare, however, for government policy to explicitly acknowledge and prioritise information and information management. Step by step, decision by decision, the everyday work of government is giving rise to a growing networked information structure, which is not based on any overall strategic agenda of, or even awareness among, political decision-makers. The vast wealth of networked information that is developing under the banner of eGovernment has come into existence without a policy blue print. As a result, its growth appears to have no "natural" limits. The fast pace of digitisation is driven by considerations of effectiveness and efficiency and, in the post 9/11 world, increasingly by considerations of security. Other considerations, such as freedom of choice and privacy, have often come under pressure when debating and implementing new applications.[8]

[1] V.J.J.M. Bekkers & S. Zouridis, "Electronic service delivery in public administration: Some trends and issues", *International Review of Administrative Sciences* 1999, 65: 183–195.

[2] J.L. Gomez-Barrosso, C. Feijoo & E. Karnitis, "The European policy for the development of an information society: The right path?", *Journal of Common Market Studies*, 2008 46 (4): 787–825.

[3] See for example D. Johnson and J. Wetmore (2009, eds.) *Technology and society. Building our socio-technical future*. Cambridge, MA: MIT Press; see also B. Latour (2005) *Reassembling the social. An introduction to Actor-Network-Theory*. Oxford: Oxford University Press.

[4] J.E.J. Prins (ed.), *Designing e-government*, The Hague 2007: Kluwer Law International.

[5] P. Dunleavy, H. Margetts, S. Bastow & J. Tinker, *Digital era governance: it corporations, the State, and e-government*, Oxford: Oxford University Press 2006.

[6] European Commission, A fine balance: privacy enhancing technologies: How to create a trusted information society—summary of conference, Brussels 2005.

[7] Prins et al. (2011) iGovernment.

[8] Prins et al. (2011) iGovernment.

Please cite this article in press as: Prins JEJ, et al., iGovernment: A new perspective on the future of government digitisation, Computer Law & Security Review (2012), doi:10.1016/j.clsr.2012.03.010

Empirically, a number of developments in the digitisation and informatisation of the public sector have taken modern government beyond the notion of eGovernment. The state's appetite for the collection and storage of personal information, the networking and pooling of personal information between various public – and sometimes also private – organisations, data mining and profiling of personal information with a view to pre-emptive policies and the growing mismatch between the horizontal flow of information in data networks on the one hand and the vertical organisation of responsibility and accountability that is characteristic of government on the other, all point towards the limits of the eGovernment paradigm. The opportunities that ICT offers, and the political opportunism and techno trust, propel these developments and take the empirical, and we argue the political, reality far beyond what may be covered under the flag of eGovernment. The developments outlined below in the following sub-sections require a different perspective, that of the iGovernment, to analyse and understand them. We will set out this perspective in section three.

2.2.1. *The ever growing bureaucratic appetite for digital data*

Public authorities have always had a natural inclination to gather information in order to govern society on the basis of that information. Torpey observed that the state first 'embraces' society in the informational sense before 'penetrating' society in order to take effective action.[9] To this end the state gathers as much information as possible, by means of a finely meshed administrative infrastructure, and then uses that information across the full breadth of government policy. The potential to 'embrace society' has increased dramatically in the digital era, and will indeed continue to do so in the foreseeable future. At the national level the number of databases and information networks have proliferated in most western societies, ranging from digital versions of 'classic' administrations (birth, marriage and death) to various new additions holding increasingly diverse and 'soft' personal information, such as indications for risk and vulnerability.

At the international and European level, there is also a noticeable trend to collect and exchange information, not in the least in the domain of 'home security'. Many new databases have been introduced or are being developed at a European level that collect, store and cross reference personal and biometric data of travellers, migrants and citizens of member states.[10] Data exchange is also a key development in the international fight against terrorism and other security related international, especially transatlantic, cooperation.[11] EU member states and the US can make generous use of these databases, either directly or indirectly, thanks to a range of treaties and official rules, complemented by what is for most – including the European Parliament– an unknown number of vague bilateral and informal agreements.[12] The European Data Protection Supervisor has warned repeatedly against the almost innate desire to expand and accumulate data, the tendency to merge policy issues and data sets – primarily security and migration policy – and the inclination to overestimate the reliability of new technologies, in particular biometrics.[13] The European Parliament has also repeatedly criticised information gathering and data exchange efforts in the area of Justice and Home Affairs, but until the Lisbon Treaty entered into effect, it did not have the formal authority to exercise democratic supervision. The Council of Ministers usually "took note" of the EP's objections without amending the proposals to which they pertained.

But it is not just governments that are collecting and producing data. Many new tools to produce, gather and disseminate information are invented outside the context of government, by both companies and private citizens. Social networking and social media, data on the behaviour of buyers and shoppers online and various sorts of personal information collected in the private sector generate a potential goldmine of digital trails and footprints.[14] That information can also be used, within the relevant margins and statutory frameworks, to satisfy government's information needs. At the same time, the mere fact that such information exists only serves to encourage those information needs. There are no natural limits to information gathering – that too is often considered on a case-by-case basis – nor are there clear guidelines on the extent to which the public and private sectors are allowed to overlap 'informationally'. Citizens thus become more and more transparent, not in the least to their own governments.

Already in 2004, Richard Thomas, the UK's Information Commissioner at the time, warned that we were 'sleepwalking into a surveillance society'.[15] On the other hand, government has so far shown little interest in interacting with citizens or even in sharing information with them, although more recent developments such as open government in the USA harbour the promise of more transparency.[16] Although

[9] J. Torpey, "Coming and going: on the state monopolization of the legitimate means of movement", *Sociological Theory* 1998, 16 (3): 239–259.

[10] D. Broeders, "The new digital borders of Europe. EU databases and the surveillance of irregular migrants", *International Sociology* 2007 22 (1): 71–92.

[11] Hert, P. de & B. de Schutter (2008) 'International Transfers of Data in the Field of JHA: The Lessons of Europol, PNR and swift', pp. 299–335 in B. Martenczuk & S. van Thiel (eds.) *Justice, Liberty, Security: New Challenges for EU External Relations*. Brussels: VUB Press, see also: Balzacq, T. (2008) 'The policy tools of securitization. Exchange, EU Foreign and Interior Policies', *Journal of Common Market Studies*, vol. 46, nr. 1, pp. 75–100.

[12] P. Hobbing & R. Koslowski, The tools called to support the "delivery" of freedom, security and justice: A comparison of border security system in the *eu and in the us*, Ad Hoc Briefing Paper, European Parliament, Directorate-General Internal Policies, Policy Department C, Citizens' Rights and Constitutional Affairs, Committee on Civil Liberties, Justice and Home Affairs, PE 2009, 410.681.

[13] European Data Protection Supervisor, *Opinion of the European data protection supervisor*, Brussels, 20 January 2006.

[14] See for example S. Baker (2008) *The Numerati*. Boston: Houghton Mifflin and V. Mayer-Schönberger (2009) *Delete. The virtue of forgetting in the digital age*. Princeton: Princeton University Press.

[15] Quoted in: I. Brown and D. Korff (2009) 'Terrorism and the proportionality of internet surveillance', *European Journal of Criminology*, vol. 6 no. 2: 119–134.

[16] See for example: Patrice McDermott (2010) 'Building open government' in: *Government Information Quarterly*, vol. 27, nr.4, pp. 401–413, for a more critical view of the programme see: Alon Peled (2011) 'When transparency and collaboration collide: The USA Open Data program', in: *Journal of the American Society for Information Science and Technology*, vol. 62, nr. 11, pages 2085–2094.

Please cite this article in press as: Prins JEJ, et al., iGovernment: A new perspective on the future of government digitisation, Computer Law & Security Review (2012), doi:10.1016/j.clsr.2012.03.010

government espouses transparency and although transparency is also on many a citizen's wish list, in practical terms the authorities seldom go much beyond good intentions. The potential is there, including in the tools made possible by ICT, but political will and resolve are lacking. As a result, transparency is often a one-way street: the citizen is transparent to government, but not the other way around.

2.2.2. *Networking the government, virtualising the citizen*

Governments increasingly let personal information on citizens flow through information supply chains and networks to support their policy processes. Storage and exchange of information between various public authorities is now faster and more efficient. In chain informatisation networks, information is passed from one organisation in the chain to the next; in proper networks, however, information is exchanged or managed collectively without it being passed along a fixed sequence of actors. Unlike supply chains, networks offer various alternative paths to information-sharing. Information can move in one direction, in different directions simultaneously, in reciprocal directions, and along multiple branches. Connections can also be strong or weak, single or multiple.[17] The dynamic, flexible and adaptive nature of a network makes it difficult to coordinate and control.[18] It is therefore also very difficult at times to decide who is responsible for specific information about citizens that circulates in networks. Who has 'ownership' and is responsible for safeguarding the accuracy of that information? Sometimes a network is also a web in which citizens can become entangled or become the victim of identity fraud.[19] In The Netherlands, even the Office of the National *Ombudsman* was unable to track down the complex chain of interactions that led to a well publicised and debated case of identity fraud – the Kowsoleea case – so that the record could be set straight. The Office concluded: "Chain computerisation can perhaps solve certain administrative problems and quicken the pace of innovation in government, but there is little reason to rely too much on its effects".[20]

The organisation of government information in networks is also at odds with the way government itself is organised. Government is a collection of semi-autonomous hierarchically organised bureaucracies (departments, agencies etc.) that are in essence vertical. In contrast, the information in networks usually flows horizontally. This inherent tension between networks and hierarchy has consequences for ensuring that the system as a whole meets vital quality standards – specifically the process-based principles of accountability and transparency. It is highly problematic if governmental information networks become so dominant, that organisations are linked in terms of information flows but not in terms of institutional arrangements. Questions relating to accountability and transparency must be taken up at the level of networks, both legally and organisationally, in order to prevent accountability and transparency from falling through the cracks of the current organisational structure. Supervision and control are largely tailored to eGovernment and are organised, as a matter of either policy or law, to the partitions of the individual policy areas. A networked government is at odds with the way in which ministries, Parliamentary committees, regulatory bodies, and legal protection and complaints procedures are set up. It is vital, however, for citizens to know who is accountable; it is vital for government to know this too so that it can safeguard the quality of information and ensure the trust of citizens in the longer term.

2.2.3. *Blurring the boundaries between the policy domains of 'service', 'care' and 'control'*

The sharp increase in data storage and computing capacity and the growing level of interoperability between different systems means that, in the *infrastructural* sense, the possibilities for networking information far exceed the classical eGovernment focus on government services. This infrastructural 'revolution' facilitates a number of policy-related and organisational developments that have radically changed the nature of digital government. Technology is no longer deployed to merely improve and streamline government *service* provision but also to gather and link information in the policy domains of *care* and *control*. Information gathered and stored for the purpose of service provision may also flow into applications and networks created in light of government policies for care and control and vice versa. Increasingly, digitised personal information plays a vital role in policies for youth care and healthcare, and has become indispensable in immigration policy and security policy, both to fight crime for counter-terrorism purposes and in the more everyday enforcement of the law (control).[21] With respect to security, information is passed not only between national public organisations but also between states and international organisations. Organisations with sometimes fundamentally different tasks sometimes share and pool information collected within their own field. The infrastructure of digitisation and interoperability makes it much easier to pool information that was originally collected and stored in what are essentially separate domains of service, care and control. In the digital age, the boundaries between these domains – which were never very sharply defined in the first place – are becoming increasingly blurred.

2.2.4. *Blurring the boundaries between the public and private sphere*

The importance of networks of actors and, in particular, information also crosses the divide between public and private information. The number of partnership and information arrangements between public and private actors is growing and gives rise to complex reciprocal information interdependencies. Private and public information flows also get blended together into these networks. The authorities are

[17] D. Barney (2004) *The network society*. Cambridge: Polity Press.

[18] M. Castells (1996) *The rise of the network society*. Cambridge MA: Blackwell.

[19] See for example: J. Whitson and K. Haggerty (2008) 'Identity theft and the care of the virtual self', *Economy and Society*. Vol. 37, nr. 4: 571–593.

[20] Nationale Ombudsman, *De burger in de ketens. Verslag van de Nationale Ombudsman over 2008*, (Year Report, 2008), The Hague 2009, p. 28.

[21] D. Lyon, *Surveillance after September 11*. Cambridge 2003: Polity Press; T. Monahan (2006; ed.) *Surveillance and security. Technological politics and power in everyday life*. London: Routledge; see also the special issue of the Web Journal *Surveillance and Society*, 2010, vol. 7, nr. 3/4 on 'Surveillance, Children and Childhood'.

Please cite this article in press as: Prins JEJ, et al., iGovernment: A new perspective on the future of government digitisation, Computer Law & Security Review (2012), doi:10.1016/j.clsr.2012.03.010

increasingly interested in the information gathered by private individuals and enterprises, and they make considerable use of such information, as is for example illustrated by the initiatives to provide passenger name records (PNR) and bank data (SWIFT) to the US.[22] At the national level, public authorities such as the Tax Services, especially the Fraud division, and the police use various sources of private information in the execution of their duties. Also, government-issued unique identifiers – such as the Dutch Citizens Service Number – are increasingly used in the private sector, irrespective of the fact this number is legally designated to be used only in government–citizen interaction.[23] Public-private ventures in the digital age, for example in public transportation or CCTV surveillance, also result in complicated systems of pooled and shared information in which it is sometimes difficult to keep the accessibility of the stored personal and location information in line with the necessity and authority to do so.[24]

2.2.5. *Profiling citizens and pre-emptive policy*

The growing number of information sources – and in particular the potential for interrelating and processing information – and the simply vast quantity of stored data means that governments increasingly (have to) make use of digital profiling techniques, and as a result group citizens into categories and profiles. Profiling plays a growing role in policy and policy implementation.[25] Categorisation of citizens becomes a dominant theme as government applies data mining and other techniques to the information it has stored in order to generate and combine a variety of information sources.[26] To some extent that is unavoidable: the amount of information stored simply exceeds human capacity, forcing government to turn to electronic processing and profiling. What this means in everyday practice, however, is that people are linked to a variety of profiles and 'data doubles'.[27] In other words, people are represented by images put together from various sources of information that sometimes take on a life of their own in the systems maintained by government (and/or business and industry).[28] Such profiles consist of information that is first *de*contextualized – taken out of the context in which it was collected – and then *re*contextualized within the context of the new composite profile. This process is naturally not an exclusively technical affair ('categories have politics'), nor is it without social implications. Being pinned down to such 'images of the future' hinders the autonomy (freedom of choice) of individuals in a way similar to the 'images from the past' that linger so long due to the ICT-revolution.[29] After all, a profile amounts to a prognosis on the future identity of an individual, based on his or her digital footprints. Government also uses such processes to anticipate the future.[30] For example, profiles and information processes play a growing role in 'preventive policing' or in the youth care sector, where information gathering and data linkages are regarded as indispensable for preventing the tragedy of child abuse.[31]

2.2.6. *An unplanned result: beyond the eGovernment paradigm*

The traditional focus, contextual frameworks and aims of eGovernment are being overtaken by day-to-day developments. The overlap between service, care and control, the circulation of personal data within networks, the merging of public and private information flows, and the tendency to use digital profiles to pursue a proactive, forward-looking policy: all these things result from a series of choices about individual applications, new systems, and decisions regarding the connections between them. Incremental change is the name of the game. Out of these 'small' decisions, a *de facto* network of information flows has evolved within the domain of government that far outstrips the policy and conceptual framework of eGovernment, even though it is constructed under that banner.

Critics condemn government's thirst for information and the rapid exchange of data between government services, drawing on images such as "Big Brother" and the "surveillance society".[32] Although change is indeed taking place at a considerable pace, such images are only marginally applicable to the situation that has arisen, mainly because they suggest an intention that is in fact absent: there is no conspiracy or intrigue involved. There is no evil genius designing the 'surveillance state'. And at the same time, that is almost exactly where the problem lies: this development is much too incremental and unaccounted for; it is too much the sum of decisions taken with respect to individual applications and policies without much thought being given to an overriding awareness of the larger whole. There is no language describing that awareness, and it certainly cannot be found in

[22] P. De Hert, & B. de Schutter, "International transfers of data in the field of JHA: The lessons of Europol, PNR and Swift", pp. 299–335 in B. Martenczuk & S. van Thiel (eds.) *Justice, Liberty, Security: New challenges for eu external relations*. Brussels: VUB Press 2008.

[23] Prins et al. 2011, *iGovernment*.

[24] Jacobs, B., 'Architecture is politics: security and privacy issues in transport and beyond', pp. 289–299 in S. Gutwirth, Y. Poullet & P. de Hert (eds.) (2010), *Data Protection in a Profiled World*, Berlin: Springer.

[25] Schinkel, W. (2011) 'Prepression: The actuarial archive and new technologies of security', *Theoretical Criminology*, vol. 15, no. 4: 365–380.

[26] M. Hildebrandt, "Defining profiling: A new type of knowledge", pp. 17–45 in M. Hildebrandt & S. Gutwirth (eds.) *Profiling the European Citizen. Cross-Disciplinary Perspectives*, Belgium/Netherlands 2008: Springer.

[27] Haggerty, K. and Erickson, R. (2000) 'The surveillant assemblage', *British Journal of Sociology*, 51(4), pp. 605–22.

[28] B.E. Harcourt, *Against prediction: profiling, policing, and punishing in an actuarial age*, Chicago: University of Chicago Press 2007; see also S. Baker (2008) *The Numerati*.

[29] See V. Mayer-Schönberger 2009 *Delete*.

[30] House of Commons Home Affairs Committee, *A surveillance society?* Fifth Report of Session 2007–08 (2 Volumes), London 2008: Stationery Office; House of Lords, *Surveillance: Citizens and the State*, London: 6 February 2009.

[31] See for example: E. Keymolen and D. Broeders (2011) 'Innocence Lost: care and control in Dutch digital youth care'. *The British Journal of Social Work*, online First, 6 December 2011.

[32] See more in general on this: D. Lyon, *The electronic eye. The rise of surveillance society*, Cambridge 1994: Polity Press. See also contributions in: M. Hildebrandt & S. Gutwirth (eds.), *Profiling the European citizen. Cross-disciplinary perspectives*, Belgium/Netherlands 2008: Springer.

Please cite this article in press as: Prins JEJ, et al., iGovernment: A new perspective on the future of government digitisation, Computer Law & Security Review (2012), doi:10.1016/j.clsr.2012.03.010

the discourse of eGovernment. Indeed, it is the eGovernment discourse that is depoliticising, instrumentalising and neutralising developments, even as the developments themselves require just the opposite. We therefore argue that a new perspective, the iGovernment, is needed to analyse and understand current developments in ICT and government and to provide a framework for future policies.

3. iGovernment

3.1. *The iGovernment paradigm*

In order properly assess the developments described above and provide guidelines for a new policy, we must begin to use the designation "iGovernment". In the words of Mayer-Schönberger and Lazer, the term iGovernment ("information Government") is a "conceptual lens that offers a complementary perspective to understand the changing nature of government and its relationship to the citizenry".[33] It therefore refers not only to the *empirical existence* of another kind of government owing to the developments we have described, but also represents another way of looking at that government. In iGovernment, the emphasis is on information flows and only in the second place on the technology that makes these information flows possible. This starting point is of great consequence, because political and public debate is dominated by ICT *projects*, and thus always starts – and often ends – with the technology or even the specific technological application.

By emphasising information flows, the conceptual lens of iGovernment shows that the trends and developments are more closely interrelated in everyday reality than a discussion of individual techniques and applications would show. The conceptual lens of iGovernment also reveals that, despite a few very modest attempts, many governments are as yet unaware of the existence and implications of an all-encompassing network of information flows, and are thus unable to set out a course accordingly. Such awareness is overdue because there are two characteristics of the *de facto* evolution of iGovernment that, when combined, are undesirable, namely that it presents a paradox of political control and that it may not know any natural limits to its growth.

3.2. *The political paradox of iGovernment*

In the evolution of digital government, many political decisions have been made along the way, yet paradoxically the political dimension has been entirely lacking in another respect. The political paradox that presses increasingly for attention is as follows: the connected reality of iGovernment has not been legitimised by explicit political decision-making, but is the result of many political and policy-related choices pertaining to individual technical applications and connections between applications and/or systems. At the same time, however, these individual choices are not simply a series of coincidences, even though ICT solutions are often presented or 'sold' as inevitabilities: they are in fact deliberate political and policy-related choices with implications far wider than the instrumental solving of problems.

Although public debate on government ICT is not rare, it tends to be focused on the multifarious ways in which systems can run aground and fail to solve the problems for which they were created. But that does not in itself constitute the real political dimension – and urgency – of iGovernment. The normative picture of what is taking shape is rather opaque. iGovernment has its origins in the actors who recognise and seize the new opportunities that ICT offers to meet their responsibilities and achieve their aims, and who develop and use the relevant tools. In many cases, they offer up a whole list of reasons for using ICT to achieve a particular policy objective, with security and effectiveness/efficiency driving the policy process onwards. At the same time, the quality of these arguments that offer ICT its thrust is rarely put seriously to the test. The same sometimes applies to the opposite corner of the normative field. Values such as privacy and autonomy (freedom of choice), which serve as a counterweight to the driving interests, can also take on a Potemkin-like quality in the hands of their proponents. Consequently, balanced assessments of the broader implications of the introduction a new ICT-application (and the new connections it entails) are hard to find. This paucity of judgment can be seen as a sign that the transparency and accountability of the political process with regard to public digital affairs is insufficient.

Most political and policy debates focus on, and result in, isolated decisions relating to separate applications, ICT programmes and policy objectives. Only rarely is any thought given to the information flows generated via these applications and how these flows and their contents take shape in the larger complex of government information processes. In many instances, the decision-making process is repeated at a later date for yet another application or new connection, or to give yet another organisation access to existing information networks, once again on an individual-case basis. In this context, function creep is a protracted but to some extent predictable process. The general public and government itself often appear to be entirely unaware of the scale on which information becomes networked and the impact thereof. Although there is often concern about separate information flows within a single policy area, about the information flow generated by a specific application, or about an individual connection, there is much less vigilance and concern about the connection of information flows further down the line, when they pass through various policy domains and are absorbed into more extensive information networks. It is precisely the absence of an overarching awareness or design of iGovernment that has allowed a complex, differentiated and sometimes contradictory accumulation of formal and informal policy development and implementation processes to arise, that differs from one measure and policy issue to the next.

3.3. *iGovernment without limits*

The accumulation of ad hoc decisions and the lack of awareness of the whole of the interconnected information networks are permitting iGovernment to evolve without boundaries or

[33] V. Mayer-Schönberger & D. Lazer, "From electronic government to information government", in V. Mayer-Schönberger and D. Lazer (eds.) *Governance and information technology: from electronic government to information government*, Cambridge, MA 2007: MIT Press, p. 5.

Please cite this article in press as: Prins JEJ, et al., iGovernment: A new perspective on the future of government digitisation, Computer Law & Security Review (2012), doi:10.1016/j.clsr.2012.03.010

limits to its growth. No one has restricted the dispersal of individual applications or the linking up of information flows, because no one has claimed stewardship of the whole. The tendency to specialise and assign issues to well-established political and administrative categories, with the associated financial frameworks, prevents a broader orientation. It is a pressing question whether and how limits can be defined to the networking of information in the public domain.

3.3.1. *Propelling forces*

Our first observation is that it is mainly interests such as effectiveness/efficiency and security that are propelling the introduction of technological applications and the connections between them. Certainly in the wake of 9/11, governments have set up many databases for security and control purposes in an effort to prevent a repeat of the disaster.[34] The dynamic relationship between Justice and Home Affairs within EU policy-making is a good example of how the protection of personal data has, time and again, been forced to give way to security concerns, with the European Parliament exercising only a minimum level of supervision. But "techno-trust" has also prevailed in recent years, pushing such popular phenomena as predictive policing and proactive management of citizens' future behaviour to the foreground. That has, in turn, put pressure on such concepts as "innocent until proven guilty"[35] and "cleaning the slate" in the criminal law.[36] The emphasis on effectiveness/efficiency and security means that fundamental interests such as freedom of choice and privacy have often been side-lined or downplayed. When it comes to individual applications and connections between databases and systems, one can always find a good reason (usually political) for letting security outweigh other considerations – necessity knows no law, after all. But if no one is aware of the result at an aggregate level, the sum total of all those individual reasons will not be taken into account. That is why the absence of limits upon the growth of information networks is most obvious when we shift our perspective from individual applications to iGovernment as a networked entity. Although the politicians and policymakers involved do weigh up the interests underlying each new application or initiative, for example security, privacy or freedom of choice, that process does not involve their assessing these interests at the level of aggregated information flows, i.e. at the level of iGovernment as a whole – even though the application will ultimately become part of the evolving iGovernment.

3.3.2. *Pooling of information*

The absence of limits can especially be gauged in the growing overlap between the policy domains of service, care and control. The emphasis on effectiveness/efficiency and security makes it appealing to break down barriers between different information domains in order to increase security, expand the scope of control, or streamline services. It also makes it easier to defend such measures politically. The domains of care and control (social safety nets) are being "mixed" in the youth care sector; control and service are crossing paths in various Internet initiatives launched by the police; and the development of new ID-card initiatives is keying into new ambitions related to both service and control.[37] Facilitated by unique ID codes (including the unique ID-numbers and biometrics), it has become possible to link a whole array of facts to a person and to share that data beyond the boundaries of what used to be isolated policy contexts and a restricted institutional setting. In everyday terms, a citizen who has filled in a form for, say, a building permission should no longer be surprised to find that information resurfacing in a tax assessment – if resurfacing is even the right word for the often subterraneous way in which information is reused.

Influenced by these trends and developments, organisations are reassessing their own role and aims. Occasionally that means that they adjust their work processes and extend their scope of activity by developing new products and services in areas of policy where they had previously not been active. Viewed from the perspective of information flows and data use, the three policy domains of care, control and service are increasingly becoming an integrated component of public administration, even though they are in no way comparable or easy to integrate in terms of policy goals, administrative infrastructure, accountability mechanisms, legal rules and other frameworks. As a result, tension arises regarding duties, powers and responsibilities, in particular because former "outsiders" (including private-sector parties) become part of the network.

4. The risks involved

iGovernment "without limits" poses certain risks and problems, not only directly, but also because opportunities to harness the potential of iGovernment are ignored or not exploited to the full. As iGovernment continues to evolve, a number of these risks must be addressed.

4.1. *Distorted images*

The first risk is that the solid basis government believes information technology will give it in a particular policy domain may turn out to be quite the opposite within the overall context of networked information systems. In the system-by-system approach described above, new applications are assessed individually and in isolated policy contexts, rather than in relation to the existing technologies and applications and the information networks in which they will be functioning. As a result, there is no clear picture of, or critical reflection on, the wider implications of any specific initiative. Ultimately, the image that government has of its own information-reality becomes distorted in this way. It fails to sufficiently identify, acknowledge and review the underlying and broader interests or the problems and risks that are bound to arise when separate initiatives are combined. Being blind to the implications of

[34] United Nations, *From e-Government to Connected Governance, United Nations e-Government Survey 2008*, New York.

[35] L. Zedner, "Pre-crime and post-criminology", *Theoretical Criminology*, 2007 vol. 11: 261–281.

[36] D. Solove, *The future of reputation, gossip, rumor and privacy on the internet*, New Haven, CT 2007: Yale University Press; V. Mayer-Schönberger, *Delete. The virtue of forgetting in the digital age*, Princeton 2009: Princeton University Press.

[37] T. Stevens, J. Elliott, A. Hoikkanen, I. Maghiros & W. Lusoli, *The State of the Electronic Identity Market: Technologies, Infrastructure, Services and Policies*, JRC Scientific and Technical Reports, Luxembourg 2010: Publications Office of the European Union.

Please cite this article in press as: Prins JEJ, et al., iGovernment: A new perspective on the future of government digitisation, Computer Law & Security Review (2012), doi:10.1016/j.clsr.2012.03.010

combining information flows may lead to unpleasant surprises. Identity fraud is one example.[38] Here we have only just begun to take stock of the underlying problems. Combining, processing and decontextualizing information are all processes that affect the quality and reliability of that information. Although the aim is to increase control, poor information quality can cloud government's view, cause its institutions and agencies to mistrust one another, leading instead to deterioration in control. There is a growing list of unfortunate cases: mistaken identity, incorrect and obsolete records that have material consequences, citizens who get bogged down in digital government networks. The risk is that politicians and policy-makers will lose the ability to orchestrate matters; they will then have to do what they can to prevent the negative impact of an ad hoc iGovernment from outweighing the benefits of ICT.

4.2. *Informational prowess without corresponding institutional adjustments*

The second risk is related to the observation that the present discourse concentrates on technological systems instead of organisational processes. The focus, in other words, is on the product, and not on the process. The debate focuses on the technical possibilities, whereas the, often plural, organisational and institutional contexts in which the technology is meant to function is insufficiently considered or fade into the background. And yet it is precisely this context that is of vital importance for ensuring that the system, once it is operational, actually meets the public's quality standards. The smooth integration (in terms of work processes, authorizations etc.) of new policy-oriented ICT systems in the setup of the organisations involved is perhaps as important as the strictly technical performance of the system in question, yet it receives much less consideration. The organisations themselves thus have an interest in attending to the 'soft' side of technological systems. But the larger issue is the position of the citizen. The development of iGovernment has involved a dramatic increase in the informational prowess of government, without offering citizens any tools to serve as a counterweight to this. For citizens caught in the sticky threads of the government's information systems, there is no institutional redress that is networked in a way similar to the information itself. Rather, the safeguards – e.g. statutory rights of access and correction of data – remain rectilinear and therefore increasingly inadequate. It will be highly problematic if the thrust of iGovernment becomes so dominant that organisations are fully connected in terms of information flows but not in terms of institutional arrangements. Questions of accountability and transparency must be taken up on the scale of the overarching iGovernment, in order to prevent these values from falling through the cracks. This involves a major (and ambitious) reworking of the legal and organisational structures meant to protect citizens against unwarranted or incorrect information use.

4.3. *Tenuous public trust*

The third risk is that a lack of boundaries will eventually undermine the citizen's confidence in government as a reliable custodian and user of information. If there is no serious consideration of the features and requirements, and also of the new risks, of iGovernment, then government becomes vulnerable in its belief that technology works perfectly. This vulnerability is only heightened by the fact that digital systems have become a vital infrastructure. Without such reflection, matters such as transparency, accountability and good commissioning practices are at risk, whereas it is precisely these qualities that promote trust in digital government. Government must be able to ensure that information flows within its own systems – and to a certain extent outside those systems – do not become so unmanageable that they end up harming citizens: or, for that matter, harming the digital reputation of government itself.

Although it is too soon to draw clear-cut conclusions, the public's trust in government is already showing some cracks. There are various examples: the campaigns of grassroots movements[39]; and the court cases initiated by individuals, organisations and even the European Parliament (e.g. in the case of Passenger Name Records). Headline cases such as the T-Mobile affair in Germany and the major breaches of data security in the UK can severely test the public's confidence in government.[40] Trust-related risks are not only a factor in the relationship between government and the citizen, but also within government itself, in particular in the relationship between policymaking and policy implementation. Both the ministries (policymakers) and the agencies and other government bodies at operational level (policy implementation) have expressed a strong need for clear guidance, not in the least to make practical management of information systems and networks possible.[41] This increasing gap between policymaking and policy implementation can be attributed to the lack of iGovernment self-awareness among policymakers and politicians. In the

[38] J. Whitson & K.D. Haggerty, "Identity theft and the care of the virtual self", *Economy and Society* 2008, 37 (4): 571–593.

[39] See in The Netherlands: <http://www.njcm.nl/site/press_releases/show/25>; <http://www.binnenlandsbestuur.nl/nieuws/2009/07/protest-tegen-opslagvingerafdruk.121883.lynkx>. Of interest is also the ruling by the Dutch Advertising Code Authority (*Reclame Code Commissie*), Amsterdam 12 January 2010, in a case against a grassroots movement that had satirically depicted the Dutch central ID-number as a tattoo on the arm, in a widely distributed *faux* government flyer, that many people (chillingly) considered real. Other examples can be found in: J.E.J. Prins, "Burgers en hun privacy: over verhouding en houding tot een ongemakkelijk bezit", pp. 1–14 in J.E.J. Prins (red.) *16 miljoen BN'ers? Bescherming van persoonsgegevens in het Digitale Tijdperk*, Leiden: Stichting NJCM-Boekerij 2010.

[40] In Germany, more than 17 million customer datasets were stolen from T-Mobile in 2006. The data included mobile telephone numbers (including unlisted ones), addresses, birthdates and e-mail addresses. All this data was offered to criminals via the Internet. There were a series of breaches of data security in the UK in recent years (i.e. secure information that was unintentionally made available in an insecure context). The cases included the loss of two computer discs storing data on 25 million child benefit recipients (November 2007); a stolen laptop with personal data on 600,000 Royal Navy recruits (January 2008); six stolen laptops with data on 20,000 patients (June 2008) (www.bbc.co.uk, consulted on 22 January 2009).

[41] This conclusion is based on numerous interviews with professionals working at various levels of the Dutch government. References to their names and affiliations can be found in the report *iGovernment* (footnote [4]).

Please cite this article in press as: Prins JEJ, et al., iGovernment: A new perspective on the future of government digitisation, Computer Law & Security Review (2012), doi:10.1016/j.clsr.2012.03.010

prevailing instrumental perception of ICT projects, there is no room for addressing the organisational difficulties that are nevertheless in full view in the daily operations of public authorities at all levels. It is crucial to address that gap, not only in order to guarantee government's (and therefore iGovernment's) ability to act decisively, but also to retain the trust of the various parties within government itself.

5. Adjusting to the reality of iGovernment

5.1. *Self-aware iGovernment*

From the analysis above follows our main conclusion: the use of ICT and, in particular, of information/information flows is bringing about major changes in both policymaking/policy implementation and social reality, which means that, in effect, a different government is now evolving. That new government is what this article calls "iGovernment". It is the nature of the new iGovernment to focus on information flows and related processes. Technology is not the leading factor here; rather, it is a facilitator. iGovernment is being created through the incremental accumulation of *de facto* initiatives that are insufficiently acknowledged as being part of a larger whole or questioned by the relevant actors. This lack of "awareness" means that the features of iGovernment are scarcely taken into account in policymaking, and that politicians and policymakers do not sufficiently realise precisely *what* is taking shape, let alone *how* they can guide that evolution in the right direction. What they require is a different perspective. The evidence indicates that, if left to its own devices, iGovernment will continue "naturally" in the same way that is has evolved so far: it will develop organically through the continuous amassing of applications and information flows. A shift in focus is needed to correct the failing awareness of this process and its consequences.

5.2. *Administrative principles for iGovernment*

Several matters are of vital importance in making the political transformation from eGovernment to iGovernment. First it requires that government becomes much more aware of various features of information than is now the case. We are referring here to *processes* of information handling and use, specifically because such processes have a huge impact on the nature and reliability of the information that feeds iGovernment. We can therefore tag three interrelated processes with 'warning flags': when information is either part of or the result of these processes, government must pay strict attention to the quality of the information and consider who bears responsibility for it. The three processes that must be flagged in this way are:

- The *networking* of information, i.e. the shared use and management of information within a network of actors.
- The *compiling* and *enhancing* of information, i.e. creating new information and profiles based on different sources in different contexts.
- Pursuing *preventive* and proactive policy based on information, i.e. actively evaluating and intervening in society based on an information-driven risk calculation.

These three information processes are the core of iGovernment and enable it to fine-tune and customise policy, obtain a comprehensive picture of the public and of the policy issues, and take proactive action where needed. At the same time, they are processes that themselves have an impact on information: they influence its nature, reliability, recognisability, contextuality and traceability. It is important to realise, much more so than is now the case, that it is precisely these three processes that are having a big impact on (a) the quality of information *content* and (b) the demands made on the *organisational* context of information flows. The quality and vulnerability of information and information processes therefore require constant, proactive vigilance throughout all branches of national government.

Government must also have a much larger measure of openness and transparency, so that citizens can be helped to understand what information is being collected on them and assist them in correcting it where necessary. At the moment, citizens are almost powerless to correct errors in personal information within the vast iGovernment information networks – errors that sometimes have huge repercussions. Moreover, iGovernment's digital "memory" demands particular attention. Both the importance of "forgetting" – people should not be judged eternally on the information that government has stored about them – and of 'remembering', i.e. government's legal obligation of archiving, require a radical cultural transformation and a firmly grounded strategy that is as yet lacking. Interestingly, the European Commission proposes to introduce the right to forget as part of its proposal for a revision of Data Protection Directive 95/46.[42]

Second, the scrupulous development of iGovernment also means being prepared to set limits to it. When iGovernment is not self-aware, its natural tendency will be to continue expanding. Although it is beyond the bounds of this article to define the limits that may be necessary – in essence, that is a political matter – it can be indicated where those limits might approximately be found. In the first place, limits flow from a more realistic balancing of the fundamental interests at stake. As noted above, the normative picture that arises form current political and policy-debates is exceedingly vague. Other inducements to limit-setting may lie in an assessment of the consequences of the intertwinement of policy domains (service, care and control), and of the diffuse boundaries between public and private information flows. What is also of great importance is the fact that the Internet has created an entirely different information environment, one from which iGovernment cannot withdraw and within which it is obliged to function. The relationship to this "world outside" also makes it very important to set well-reasoned limits, as was made very clear by the *Wikileaks* affair.

Thirdly, prudent efforts to build iGovernment require changes at an institutional level. A government that has taken

[42] COM (2012) 11 final, Brussels January 25, 2012. Article 17 provides the data subject's right to be forgotten and to erasure. See also: Paragraph 3.4 (p. 10) of the Proposal's Explanatory Memorandum. For a discussion of the proposal, see: Christopher Kuner, "The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law", *Privacy and Security Law Report*, 11 PVLR 06, 02/06/2012. 1.

Please cite this article in press as: Prins JEJ, et al., iGovernment: A new perspective on the future of government digitisation, Computer Law & Security Review (2012), doi:10.1016/j.clsr.2012.03.010

on another guise in the digital world must also make the necessary organisational changes. When government is linked up in terms of its information flows, the accountability structure must fit in with this new reality and operate with the necessary efficiency. "iGovernment self-awareness" is not just a status to enjoy, but rather an ongoing challenge that must ultimately be ingrained in every tier of government. The key mission here is that government improves its accountability vis-à-vis individuals who become entangled in information networks. Also, it must increase the transparency of iGovernment vis-à-vis citizens. The puzzle must be solved of how to organise the protection of citizens in a fashion that is as networked as everything else. Governments in all modern countries face a crucial challenge: they must be willing and able to move the focus of debate from technology and individual applications to a new level, i.e. to interrelated information processes and linked information.

J.E.J. Prins (*J.E.J.Prins@uvt.nl*) *Member CLSR Editorial Board. Professor of law and informatisation at Tilburg University (Tilburg Institute for Law, Technology, and Society), The Netherlands; Council Member of the Scientific Council for Government Policy (Wetenschappelijke Raad voor het Regeringsbeleid – WRR), The Hague, The Netherlands.*

D. Broeders *Senior staff member Scientific Council for Government Policy (WRR), researcher Department of Sociology, Erasmus University Rotterdam, The Netherlands.*

H.M. Griffioen *Staff member Scientific Council for Government Policy (WRR) also affiliated with the Faculty of Law, Leiden University.*

Please cite this article in press as: Prins JEJ, et al., iGovernment: A new perspective on the future of government digitisation, Computer Law & Security Review (2012), doi:10.1016/j.clsr.2012.03.010